UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,839,437 B1 Page 1 of 3
APPLICATION NO. : 09/494876
DATED : January 4, 2005
INVENTOR(S) : Crane et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

The title page showing the illustrative figure should be deleted to be replaced with the attached title page.

The drawing sheet, consisting of Fig. 5, should be deleted to be replaced with drawing sheet, consisting of Fig. 5, as shown on the attached page.

Col. 12, line 30: after "routines are" delete "access" and insert --accessed--.

Col. 13, line 9: after "includes" delete "parameter" and insert --parameters--.

Signed and Sealed this

Twenty-fourth Day of October, 2006

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

(12) **United States Patent**
Cranc et al.

(10) **Patent No.: US 6,839,437 B1**
(45) **Date of Patent: Jan. 4, 2005**

(54) **METHOD AND APPARATUS FOR MANAGING KEYS FOR CRYPTOGRAPHIC OPERATIONS**

(75) Inventors: **Michael A. Crane**, Austin, TX (US); **Sohail H. Malik**, Galthersburg, MD (US); **John Clay Richard Wray**, Chelmsford, MA (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/494,876**

(22) Filed: **Jan. 31, 2000**

(51) **Int. Cl.**^{7} **H04L 9/00**
(52) **U.S. Cl.** **380/286**; 380/277; 380/282; 713/167; 713/171; 713/172
(58) **Field of Search** 380/286, 282, 380/277, 45; 713/175, 187, 159, 167, 171, 172, 163

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,513,261	A	*	4/1996	Maher	380/277
5,748,736	A	*	5/1998	Mittra	713/163
6,625,734	B1	*	9/2003	Marvit et al.	713/201
6,711,264	B1	*	3/2004	Matsumoto et al.	380/283

OTHER PUBLICATIONS

Sun Microsystems. "How to Implement a Provider for the Java Cryptography Architecture", Sep. 1998.*
Sun Microsystems. "keytool—Key and Certificate Management Tool", 1998 (part of Java 1.2).*

Wood, Matthew. "The CSSM PKCS #11 Adaptation Layer", Oct. 1998.*

Knudsen, Jonathan, Java Cryptography, O'Reilly & Associates 1998, p. 79.*

Intel Corporation, Common Security Services Manager. Service Provider Interface (SPI) Specification, Release 1.0, Oct. 1996.*

Intel Corporation,"Intel's Common Data Security Architecture", Dec. 11, 1996.*

Sun Microsystems, Java Platform 1.2 (3 documents): "jarsigner–JAR Signing and Verification Tool", "Java Platform 1.2 API Specification: Class KeyStore" and "The Java Virtual Machine Specification", § 2.10 and § 3.6.*

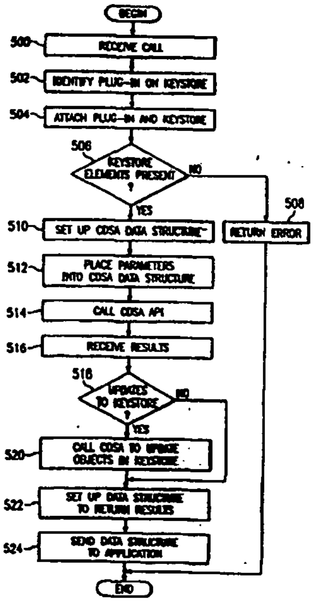
* cited by examiner

Primary Examiner—Gregory Morse
Assistant Examiner—Michael J. Simitoski
(74) *Attorney, Agent, or Firm*—Duke W. Yee; Jeffrey S. LaBaw; Stephen J. Walder, Jr.

(57) **ABSTRACT**

A cryptographic system for use in a data processing system. The system includes a security layer and a plurality of cryptographic routines, wherein the plurality of cryptographic routines are accessed through the security layer. Also included is a keystore and a keystore application program interface layer coupled to the security layer. The keystore application program interface layer receives a call from an application to perform a cryptographic operation, identifies a routine, calls the routine to perform the cryptographic operation, receives a result from the routine, and returns the result to the application.

24 Claims, 3 Drawing Sheets


BEGIN
500
RECEIVE CALL
502
IDENTIFY PLUG-IN OR KEYSTORE
504
ATTACH PLUG-IN AND KEYSTORE
506
KEYSTORE ELEMENTS PRESENT ?
NO
YES
508
RETURN ERROR
510
SET UP CDSA DATA STRUCTURE
512
PLACE PARAMETERS INTO CDSA DATA STRUCTURE
514
CALL CDSA API
516
RECEIVE RESULTS
518
UPDATES TO KEYSTORE ?
NO
YES
520
CALL CDSA TO UPDATE OBJECTS IN KEYSTORE
522
SET UP DATA STRUCTURE TO RETURN RESULTS
524
SEND DATA STRUCTURE TO APPLICATION
END

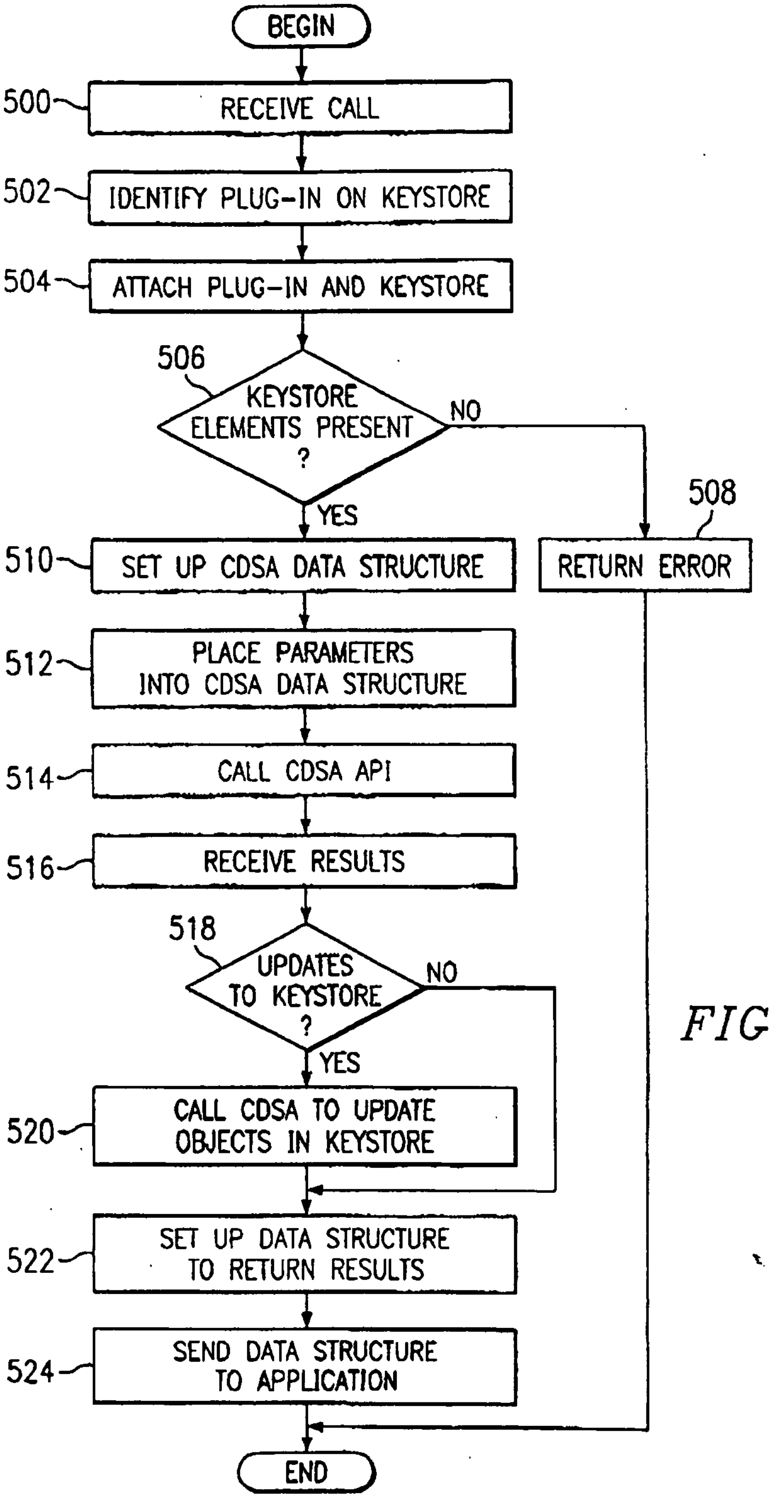

BEGIN
500
RECEIVE CALL
502
IDENTIFY PLUG-IN ON KEYSTORE
504
ATTACH PLUG-IN AND KEYSTORE
506
KEYSTORE ELEMENTS PRESENT ?
NO
YES
508
RETURN ERROR
510
SET UP CDSA DATA STRUCTURE
512
PLACE PARAMETERS INTO CDSA DATA STRUCTURE
514
CALL CDSA API
516
RECEIVE RESULTS
518
UPDATES TO KEYSTORE ?
NO
YES
520
CALL CDSA TO UPDATE OBJECTS IN KEYSTORE
522
SET UP DATA STRUCTURE TO RETURN RESULTS
524
SEND DATA STRUCTURE TO APPLICATION
END

FIG. 5